REMARKS

Claims 1-11 and 19-20 were rejected under 35 USC 102 based on Vaidya. Claims 12-13 were rejected under 35 USC 102 based on Hodges. Claims 14-18 were rejected under 35 USC 102 based on Munson et al. Claims 1-20 have been canceled above, and new claims 21-32 have been presented. Applicants distinguish the pending claims 21-32 from the cited art based on the following.

New claim 21 recites automatically ordering of the stored plurality of intrusion signatures based on how many times each of the intrusion signatures matched the system event signatures, such that the intrusion signature matching the most system event signatures is first in the order; and subsequently comparing a signature of a subsequent system event with the plurality of intrusion signatures in the order. Thus, the order of the signatures in the list typically impacts the time required to match a system event signature to a signature on the list. Because of the ordering recited in claim 21 based on past experience, there is a greater likelihood that a subsequent system event signature will match a signature earlier on the list than later, and this statistically reduces search time through the order to find a match. This is not taught or suggested by the Prior Art. Vaidya discloses that an attack signature profile might include expressions A, B and C. Vaidya also discloses an expression list, for example, including expressions A, B and C. However, the ordering of Vaidya's list is not changed based on how many times there is a match to each expression, and there is no suggestion of this. Moreover, Vaidya does not disclose that past experience is relevant to subsequent events. Therefore, no rejection of claim 21 would be warranted under 35 USC 102 or 35 USC 103.

Claims 22 and 23 depend on claim 21. Independent claim 24 distinguishes over Vaidya for the same reasons that claim 21 distinguishes thereover, and claims 25 and 26 depend on claim 24.

New claim 27 recites automatically detecting a subsequent system event having a signature; and comparing the subsequent system event signature with the plurality of intrusion signatures, and if no match is found, storing the subsequent system event signature in association with the plurality of intrusion signatures and also storing an indication that no corrective action is needed in response to detection of the subsequent system event. Paragraphs 0207-0209 of Hodges cited by Examiner against original claim 12 are concerned with profile attributes of a user and not signatures of an intrusion. Moreover, these user profile attributes of Hodges are not compared to determine whether a corrective action is needed in response to detection of a subsequent system event as recited in new claim 27. Moreover, the cited teachings of Hodges are concerned with non analogous art, i.e. authentication of users, and not intrusion detection.

Munson teach:

> "The execution profile comparator determines any difference (i.e. a differenced profile) between a current execution profile 501 most recently obtained from first profile transducer 202 and a nominal execution profile obtained from nominal profiles data 506, which represents the steady-state behavior of the software system with no intrusive activity. The initial profiles data are initially established by a calibration process that is implemented by running the program in a calibration mode in which the program is run through as many of the functions and operations performed during a nominal operational phase. A nominal activity profile and boundary conditions for variations during this nominal operational phase are accumulated during this calibration mode. The nominal profile is subsequently modified by a user (or administrator), if during normal operation of the program an alarm is raised, but it is determined that no intrusion has occurred." Column 4 lines 27-43.

While Munson teaches modification of the nominal profile to better match normal conditions, Munson does not teach: storage of signatures that do not represent intrusions, in association with signatures that represent intrusions, and storing an indication that no corrective action is needed in response to detection of the subsequent system event. Moreover, Munson detects intrusion in a different manner than that of the present invention. Munson detects intrusions by monitoring the modules that are executed and their frequency, and detecting differences in subsequent operation which indicate an intrusion. This is fundamentally different than searching through a list of intrusion signatures for a matching signature. Therefore, no rejection of claim 27 would be warranted under 35 USC 102 or 35 USC 103.

Claim 28 depends on claim 27. Independent claim 29 distinguishes over Hodges for the same reason that claim 27 distinguishes over Hodges. Claim 30 depends on claim 29.

Independent claim 31 distinguishes over Hodges for the same reason that claim 27 distinguishes over Hodges. In addition claim 31 recites subsequently ordering the stored plurality of intrusion signatures and the one system event signature based on the respective number of times that have been recorded for the plurality of intrusion signatures and the one system event signature, such that the signature for which the most number of times has been recorded is first in the order; and subsequently comparing a signature of a subsequent system event with the signatures in the order until finding a match between the subsequent system event signature and one of the signatures in the order. Consequently, independent claim 31 distinguishes over Vaidya for the same reason that claim 21 distinguishes over Vaidya, and also distinguishes over Vaidya because the one system event signature (not corresponding to an intrusion) is included in the order. If this one system event occurs relatively frequently, its signature will be near to the beginning of the order. This will reduce search time through the list because the search can terminate when the one system event signature is encountered without searching the remainder of the list. Therefore, no rejection of claim 31 would be warranted under 35 USC 102 or 35 USC 103.

Independent claim 32 distinguishes over Hodges and Vaidya for the same reason that claim 31 distinguishes over Hodges and Vaidya.

Based on the foregoing, Applicants request allowance of the present patent application as amended above.

Respectfully submitted,

Arthur J. Samodovitz
Reg. No: 31,297

Dated: January 9, 2006
Telephone: 607-429-4368
Fax : 607-429-4119